UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation	Action Nos. 13-MAG-2814, M9-150

DECLARATION OF JOSEPH V. DEMARCO

I, **JOSEPH V. DEMARCO, ESQ.**, pursuant to Title 28, United States Code, Section 1746, declare as follows:

1. I am a partner in the law firm of DeVore & DeMarco LLP, an attorney in good standing to practice law in the State of New York, and am admitted to practice in the United States District Court for the Southern District of New York.

2. At the request of Microsoft Corporation ("Microsoft"), I have prepared this Declaration in connection with the above-captioned litigation. Specifically, in order to aid this Court in a proper resolution of the issues in controversy, Microsoft has requested that I provide my insight and analysis concerning certain practices and procedures related to the preservation of electronic evidence held by electronic communications service providers located outside the United States pending the fulfillment of requests made under Mutual Legal Assistance treaties ("MLATs") and Letters Rogatory for such evidence by the U.S Department of Justice (the "DOJ").

I. SUMMARY

3. I have reviewed the April 25, 2014, Memorandum and Order of U.S. Magistrate Judge James C. Francis IV (1:13-mj-02814-UA, No. 5), Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion dated June 6, 2014 (1:13-mj-02814-UA, No. 15), the Government's Brief in Support of the Magistrate Judge's Opinion filed on July 9, 2014 (1:13-mj-02814-UA, No. 60), the Council of Europe's Convention on Cybercrime, and the related supporting materials cited herein. Based on my experience and expertise in the field of electronic evidence preservation and collection, as described below, and my review of the aforementioned documents, I am aware that there are several methods of evidence preservation that are used by the DOJ for the purpose of quickly, effectively, and efficiently ensuring that electronic communications and other digital evidence located abroad are preserved pending the execution of formal legal process to obtain such evidence.

II. QUALIFICATIONS

4. I am a founding partner at the law firm of DeVore & DeMarco LLP, where I specialize in counseling clients on complex issues involving information privacy and security, computer intrusions, theft of intellectual property, on-line fraud, and the preservation and collection of digital evidence. From 1997 to 2007, I served as an Assistant United States Attorney for the Southern District of New York, where I founded and headed the Computer Hacking and Intellectual Property ("CHIPs") program, a group of prosecutors dedicated to investigating and prosecuting violations of federal cybercrime laws. From January, 2001, until July, 2001, I served as a visiting Trial Attorney at the Computer Crime and Intellectual Property Section of DOJ in Washington, D.C. ("CCIPS"). At CCIPS, among other things, I was responsible for assisting federal and state prosecutors throughout the United States as well as

foreign prosecutors and other law enforcement officials in the preservation and collection of electronic evidence from, among other entities, Internet Service Providers ("ISPs") located inside and outside the United States. In these roles, I personally prepared and facilitated, and was aware of the preparation and facilitation by other law enforcement officials, of emergency requests for electronic evidence, including requests for the preservation and collection of electronic evidence from ISPs and providers of electronic communications services. In addition, I was also responsible for working on CCIPS' policy-related efforts concerning the Council of Europe's (then draft, now final) Convention on Cybercrime (the "Budapest Convention").

5. Since 2007, in my private practice, I have regularly counseled clients on the preservation and collection of electronic evidence in criminal and civil litigations and investigations both domestically and internationally. This has included requests for the emergency preservation of electronic evidence from electronic communications service providers.

6. Since 2002, I have served as an Adjunct Professor at Columbia Law School, where I teach the upper-class Internet and Computer Crimes seminar. I have spoken throughout the world on a range of cybercrime, digital evidence collection and preservation, cloud computing, e-commerce law, and IP rights enforcement issues. Domestically, I have lectured on the subject of cybercrime and electronic evidence gathering at Harvard Law School, the Practicing Law Institute ("PLI"), the National Advocacy Center, and at the FBI Academy in Quantico, Virginia. Internationally, I have lectured on these subjects to law enforcement officials and lawyers in Europe, Asia, and the Middle East. I am on the Board of Advisors of the *Center for Law and Information Policy* at Fordham University School of Law, and am a member of the Professional Editorial Board of the *Computer Law and Security Review* published by

Elsevier. I am also listed in *Chambers USA: America's Leading Lawyers for Business* guide as a leading lawyer nationwide in Privacy and Data Security, and am a *Martindale-Hubbell* AV-rated lawyer in the areas of Computers and Software, Litigation and Internet Law.

7. As a former federal prosecutor and as an attorney in private practice, I have had extensive experience throughout my career with complex issues relating to electronic evidence preservation, collection, and spoliation. For example, as the head of the CHIPs program in the Southern District of New York, I was responsible for supervising and advising Assistant United States Attorneys in the District in a broad variety of criminal cases on how to find and collect electronic evidence -- such as the content of e-mails and associated account transmission and subscriber records -- from a wide range of sources, both domestically and internationally. In particular, I regularly reviewed applications for search warrants, court orders, MLAT requests, as well as grand jury subpoenas and administrative subpoenas which called for the production of various forms of electronic evidence. In addition, while at CCIPS, I was responsible for advising foreign law enforcement officials from numerous countries regarding evidence preservation techniques and strategies as they related to U.S. law, as well as with applicable evidence retention, preservation, and access policies and practices of ISPs based in the United States. I provided this advice and assistance in cases involving routine requests for electronic evidence as well as in exigent circumstances where the need for very rapid and efficient action was frequently of paramount importance.

8. In addition to my experience in government, in private practice I have continued to be frequently called upon to provide advice on the preservation and collection of digital evidence. The need for this assistance arises in cases implicating both criminal statues as well as civil causes of action; not infrequently, these requests are either extremely time-sensitive

and/or involve high-stakes digital evidence preservation and collection issues. For example, I have provided advice related to the preservation and collection of e-mail communications and other electronic evidence in cases involving extortion, computer hacking, theft of trade secrets, illegal password trafficking, copyright infringement, and harassment and cyber-stalking, among others. I have also frequently been involved in representing clients who have been asked to provide digital evidence and other assistance to the government in criminal as well as intelligence-related investigations.

9. Based on the above experience, I am familiar with requests to seek evidence preservation and collection from ISPs and similar entities, including through the assistance of foreign law enforcement officials. I am also aware that law enforcement officials outside the United States regularly cooperate with federal and state criminal investigators in the United States to achieve the preservation of electronic evidence for use in investigations and prosecutions. This cooperation both complements and reinforces the MLAT and Letters Rogatory framework and includes (a) direct law-enforcement-to-law-enforcement informal cooperation, (b) a more formal "24/7" network, and (c) the Budapest Convention discussed below.

III. INTERNATIONAL EVIDENCE PRESERVATION IN CRIMINAL INVESTIGATIONS

10. Because of its nature, electronic evidence often can be lost if it is not secured in a timely and efficient manner. Partly as a result of this, in my experience, law enforcement officials in various countries communicate with each other directly in cases involving electronic evidence in order to locate, preserve, and collect such evidence. Based on my experience, such direct cooperation is particularly close between United States and Western

European law enforcement officials, as well as between law enforcement officials in the United States and those of English-speaking nations throughout the world.

11. In addition to the direct law-enforcement-to-law-enforcement cooperation noted above, since at least 2001, the DOJ has maintained a "24/7 Network" list of emergency law enforcement contacts committed to assist in the preservation of digital evidence across international borders consistent with national legislation. As its name suggests, this list allows for around-the-clock contact among participants to achieve electronic evidence preservation. The list consists of representatives from dozens of countries around the world.

12. Moreover, on December 29, 2006, the United States ratified the Budapest Convention. Notably, Article 29 of the Convention requires that signatory countries implement laws so that foreign governments can request the preservation of electronic data inside their borders and thus ensure that requested data is "not [] altered, removed or deleted during the period of time required to prepare, transmit and execute a request for mutual assistance to obtain the data."[1] The Convention contemplates that, following preservation pursuant to its mandate, access to data by a foreign nation shall proceed according to established international legal process. Notably, international preservation requests as contemplated by the drafters are quite common.[2] Noteworthy too is that the Convention affirms and supports the 24/7 Network

---

[1] *See* Council of Europe, *Explanatory Report to the Convention on Cybercrime,* available at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (last visited July 22, 2014).

[2] *See* Cybercrime Convention Committee, *Assessment Report: Implementation of the Preservation Provisions of the Budapest Convention on Cybercrime*, at 17, 49 (January 25, 2013), available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf (last visited July 22, 2014), (noting that as of 2012 the "U.S. sends and receives hundreds of preservation requests per year").

discussed above.[3] To be clear, these mechanisms supplement the direct law-enforcement-to-law-enforcement communications which I describe in paragraphs 10 and 11, above.

13. Through law-enforcement-to-law-enforcement cooperation, the 24/7 Network, and the Budapest Convention, U.S. law enforcement officials and their foreign counterparts regularly preserve electronic evidence on behalf of one another, including evidence at ISPs, across international borders.

14. The government states in its brief that MLATs "typically take[] months to process." Gov't Br. 25. Based on my knowledge and experience, there is no "one size fits all" period of time in which MLATs are executed. Rather, the speed at which an MLAT is acted upon is a function of the urgency and priority of that request to law enforcement officials. Many MLATs submitted by United States officials to foreign counterparts are not especially time sensitive or urgent, and part of the period associated with receiving evidence via an MLAT consists of the time that DOJ takes to prepare and transmit the MLAT to foreign counterparts. This involves work at the local United States Attorney's office and/or prosecuting unit at DOJ and, subsequently, at the Office of International Affairs, which is the central office at DOJ to which draft MALTs are regularly forwarded for review, comment, approval, and ultimate transmittal abroad. Importantly, however, in my experience, DOJ officials and relevant foreign

[3] *Id.* at 4, 12.

executing officials can, and regularly do, move with great alacrity and efficiency in processing, transmitting, and responding to high-priority MLATs.

15. I declare under penalty of perjury that the foregoing is true and correct.

Dated: New York, New York
July 24, 2014

Joseph V. DeMarco